DPM host level protection of VMware VMs

System Center 2012 R2 Data Protection Manager (DPM 2012 R2) with Update Rollup 11 (UR11) or later adds support for protecting host level backup of virtual machines running on VMware 5.5 and 6.0 servers. This is accomplished by using VMware APIs over the network and does not require that a DPM agent be installed on the VMware ESXi hosts or vCenter servers.

**IMPORTANT NOTE:** DPM 2016 will add support for VMware protection in Update Rollup 2 (DPM 2016 UR2). During the upgrade, you will receive a message stating that VMware protection was detected and the console will not run until DPM 2016 UR2 is installed. Once DPM 2016 UR2 is installed, the console will work and VMware protection will resume.

DPM agentless VMware VM backup

DPM is a true agentless VMware VM backup solution. There is no need to install a DPM agent on any vCenter or ESX servers to start backup protection of virtual machines. The DPM server will communicate with vCenter or ESX hosts directly using SOAP calls over HTTPS to perform backups. To start protecting VMware hosted VMs, you first need to add vCenter or ESX servers to DPM by providing the IP address or FQDN of the vCenter or ESX server along with proper login credentials to authenticate with VMware.

The diagram below illustrates communications between DPM and VMware performed by DPMRA. The DPM Engine is not directly involved with any communications between vCenter or ESX or ESXi hosts.

Note that the destination files are vhdx files which are native Hyper-V format which allows for DPM Item Level Recovery (ILR) from protected Windows guests.

If the ESXi servers are managed by vCenter, the vCenter should be added to DPM. Otherwise, add the ESXi server to DPM. Below are examples of how DPM can enumerate VMs running in large data center
deployments using vCenter or by protecting individual VMware ESXi servers that are not being managed by vCenter.
Keep in mind that it is possible that both vCenter and an ESX host could accidentally be added to a DPM server, and in that case DPM would show both views of the same VMs as seen below.

To prevent this, if the ESX host is being managed by vCenter, Lockdown mode can be enabled on that ESX host. Lockdown mode prevents remote users from logging directly into the host, meaning that the host will only be accessible through the local console or an authorized centralized management application like vCenter. You can change the lockdown mode setting from the vSphere web UI by navigating to Hosts and Clusters and selecting the ESX host, then changing LockDown to enabled.

VMware credential management

Because DPM’s VMware backup is an agentless backup solution, DPM performs backups by interacting with vCenter/ESX servers remotely. This is achieved by DPM remotely authenticating with the VMware server. This authentication is required and performed every time DPM interacts with VMware servers. DPM securely stores the required credentials locally in Windows Credentials Manager and uses them whenever needed. Since these credentials can be changed periodically, and because a datacenter may have multiple vCenters or ESX hosts that need different credentials, DPM has built-in credentials management. However, before creating a credential in DPM, the VMware user account used for the credential must have certain privileges.

Required privileges

The required VMware user privileges are in the following table:
### Required User Privileges

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore.AllocateSpace</td>
<td></td>
</tr>
<tr>
<td>Global.ManageCustomFields</td>
<td>(Manage custom attributes)</td>
</tr>
<tr>
<td>Network.Assign</td>
<td>(Assign network)</td>
</tr>
<tr>
<td>VirtualMachine.Config.AddNewDisk</td>
<td></td>
</tr>
<tr>
<td>VirtualMachine.Config.AdvancedConfig</td>
<td>(Advanced)</td>
</tr>
<tr>
<td>VirtualMachine.Config.ChangeTracking</td>
<td>(Disk change tracking)</td>
</tr>
<tr>
<td>VirtualMachine.Config.HostUSBDevice</td>
<td></td>
</tr>
<tr>
<td>VirtualMachine.Config.SwapPlacement</td>
<td>(Swap file placement)</td>
</tr>
<tr>
<td>VirtualMachine.Interact.PowerOff</td>
<td></td>
</tr>
<tr>
<td>VirtualMachine.Inventory.Create</td>
<td>(Create new)</td>
</tr>
<tr>
<td>VirtualMachine.Provisioning.DiskRandomRead</td>
<td>(allow read-only disk access)</td>
</tr>
<tr>
<td>VirtualMachine.State.CreateSnapshot</td>
<td>This is under Snapshot Management</td>
</tr>
<tr>
<td>VirtualMachine.State.RemoveSnapshot</td>
<td>This is under Snapshot Management</td>
</tr>
</tbody>
</table>

These privileges are assigned to **Roles** in vCenter or the vSphere client, and can be created or managed under **Administration -> Roles**. Once you create a role with the privileges above, you can assign that role to an existing or a new user account.

### Creating new role for an individual ESXi server

The steps below demonstrate how to create a new role for an individual ESXi host. If the host is managed by vCenter, go to the **Creating a new role for vCenter** section.

1. Connect to the ESXi host using the vSphere client.
2. In the vSphere client while on the Home screen click on the Inventory icon.
3. Under the Local users & groups tab, right-click and Add a new user.
4. Fill out the form and select a strong password. In this example the user name is DPMBKUP.

To add a dedicated role and assign required privileges, complete the following:

1. In the vSphere client while on the Home screen, under Administration click on the Roles icon.
2. Click on the Add Role button.
3. In the example below, the DPMBKUP role is created. Select the required privileges from the list of required user privileges above and save them.

Now assign permissions to the DPMBKUP user account:

1. From the vSphere client screen, select the Inventory icon.
2. Click on the Permissions tab.
3. Right-click and select Add permissions...
4. In the new **Assign Permissions** dialog box, press **Add**...

5. Select the DPMBKUP user then press the **Add** button, then click **OK**.

6. Once the DPMBKUP user is added, select the DPMBKUP role from the **Assigned Role** drop down list. This will give that user account the required privileges to perform backups and restores.
Creating a new role in vCenter

In large VMware deployments, the ESXi hosts will be managed by one or more vCenter servers. DPM can protect all the VMs through the vCenter server instead of having to add each ESXi host to protection. To create a new role with the required privileges using the vCenter console, perform the following steps:

1. Connect to the vCenter server using the vSphere client and go to the Home screen.

2. Under Administration, click on the Roles icon.

3. Click the plus (+) sign to create a new role.
4. In the **Create Role** dialog, enter a role name, then locate and enable the required privileges as shown in the required user privileges table above. Click **OK** to save.

5. After the new role is saved, go back to the **Home** menu and click the **Hosts and Clusters** icon under **Inventories**.

6. Select **Manage**, then go to the **Permissions** tab to show a list of users/groups.
7. Click on the plus (+) sign to add the role to an existing user that will be used for the DPM credentials. The Add Permission dialog will open.
8. Select the DPMBKUP role created earlier from the Assigned Role drop down list.

9. Click Add... to select the user to add to this role, then add the user and click OK.
10. Once added, that user account can then be used for DPM credentials.

11. On the DPM server, enter that username and password:
Creating VMware credentials

VMware credentials can be managed by selecting the **Manage VMware credentials** option as shown below. You can add credentials here before adding a VMware server, or you can specify credentials while adding a VMware server.

**NOTE:** After installing DPM 2012 R2 UR10 or later, the **Agents** link under **Management** has been changed to **Production Servers**. This was necessary because VMware servers do not require agents. A new **Type** column was added to the protected servers page to differentiate between Windows servers and VMware servers.

The **Add Credential** screen will be displayed to enter a friendly name of the credential, a description, the user ID and password. This new credential can be used when adding vCenter or ESXi hosts to DPM.
When adding a new server for protection and selecting VMware, the wizard will allow you to select a pre-existing credential, or you can create a new credential on the fly while adding the server.
Modifying the credentials of a VMware server

Most organizations need to update credentials for security reasons or when personnel changes. When VMware server credentials are changed, credentials that are used by DPM also need to be updated. There are two methods to change credentials used by DPM to communicate with a VMware server:

1. You can change the username and password associated with the current credential used by one or more server.
2. You can create or select a completely different credential to use for one or more servers.

Changing an existing credentials **User ID** or **Password**:
Changing a credential used by a vCenter or ESX server:

Notes on credentials:

- A single credential can be used for authenticating multiple VMware servers.
- Credential details include credential description, login name and password. Once it is updated, all VMware servers that are using this credential will be authenticated with the new credentials.
• A credential cannot be deleted if it is currently being used by any VMware server’s authentication setting. Before attempting to delete a credential, change all VMware servers using that credential to use a different credential.

• VMware credentials are stored locally on the DPM server using Windows Credential Manager (CredMan). The passwords are stored encrypted in the CredMan database. The friendly credential’s name, user name and description are stored in the DPMDB in a table called tbl_IM_Credentials. Should the DPM server need to be rebuilt and the DPMDB restored, only the password will need to be re-entered.

Adding a VMware server
First step in protecting a VMware server is to add it to DPM server. VMware server authentication can be done by two step process.

Step 1: Setting up secure communication between DPM and the VMware server
To communicate securely with a VMware server, a certificate is used. DPM connects to VMware via the HTTPS protocol, so the certificate that is installed on VCenter or ESX host must be trusted by the DPM server. Each ESX server will have its own certificate, however if the vCenter server is added as a protected server, you do not have to deal with the certificates of all the other ESX servers that are managed by that vCenter server.

If a certificate is not deployed on vCenter or the ESX hosts, or you did not install the certificate on the DPM server, you can disable secure communication between DPM and VMware via the registry. Currently, this is a global setting and will disable all secure authentication between DPM and the VMware servers. Even if certificates are deployed on one or more ESX hosts and the DPM server, they will not be used by DPM if this registry setting is enabled.

To disable secure communication via the registry, copy and paste the following text into a file called DisableSecureAuthentication.reg on DPM sever and double-click the file to add the entry to the local registry.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\VMware]
"IgnoreCertificateValidation"=dword:00000001
```

That will create the following registry value:
Step 2: Add the VMware server to DPM

Add a new VMware server by selecting the **Production Server** tab, then **Add** as shown below.

The **Production Server Addition Wizard** allows multiple VMware servers to be added to the DPM server at one time. Each server added can share the same credentials or use separate credentials as needed.
Each vCenter or VMware server that needs to be added should have the following details:

1. The FQDN of the vCenter, the FQDN of the VMware server, or the IP address of the server.
2. The SSL port used to communicate with the VMware server. Because HTTPS is used, DPM needs to know the SSL port that the VMware server is configured to use. If the VMware servers is not explicitly configured with a non-standard SSL port, simply use the default port which is 443.
3. The credential needed to authenticate with the VMware server. If the required credential is not yet added to DPM, create a new credential by selecting Add New Credential as shown below.
After adding the vCenter or ESXi servers, proceed through the wizard to completion.

If the credentials are incorrect, or if there is no valid trusted certificate, or if the ESX server has the lockdown option enabled because it’s being managed by vCenter, you will get an error 0x80990EF2 or 0x8099DEF2 when trying to add the ESX server to DPM. Check the DPMRACurr.errlog to see what the true cause is for the error and correct it accordingly. Here is an example:

**VMware version:** 5.5.0  
**Error:** Data Protection Manager Error ID: 33623  
Unable to communicate with VMware Server 172.29.11.229.  
**Detailed error code:** Internal error code: 0x80990EF2  
**Recommended action:** Please ensure that the specified VMware server is up and running and reachable from DPM Server.  
Also, ensure that right credentials are specified for interacting with specified VMware Server.

Protecting VMware VMs

DPM supports both application consistent and crash consistent backups. To obtain application consistent backups, you must install the VMware tools on the guest. VMware tools is an optional free set of drivers and utilities that interact between the host and guest operating systems and support taking snapshots inside guests that support snapshots. The VMware tools are equivalent in nature to the Windows Hyper-V Integration components. If the VMware tools are not installed, backups should succeed, however they will only be crash consistent.

You can install the VMware tools for guests using either the vSphere web client or vCenter by clicking on the link to install the tools, then following the directions in the resulting dialog.
DPM can protect VMware guests hosted on both NFS and VMFS storage. Fault tolerant clustered VMs are supported, however VMs hosted on shared disk clusters are not. Change tracking on shared disks is not supported by VMware.

Before starting protection in DPM, disk storage need to be added to DPM as documented in Adding Storage to DPM. After adding storage to DPM, VMware VMs can be protected by going to the Protection tab and expanding the VMware servers tree as shown below.

If there are Inquiry errors, they will be displayed in a DataSource enumeration details popup with a list of errors. Possible reasons are an invalid certificate, login failures or permissions issues. In the screenshot below, the credentials used were invalid at the time of the inquiry. There is no need to look at the logs for this failure because the details show InvalidLogonFault.
Differences between protecting VMs hosted on NFS and VMFS storage

**Initial Replica (IR):** For VMFS hosted VMs, DPM will use a VMware API call to ask for a list of allocated blocks inside the vmdk files. DPM will only read and transfer those allocated blocks and write them to a corresponding vhdx file on the replica volume. DPM uses the vhdx format so that item level recovery can be performed for Windows guests.

For NFS hosted VMs, the VMware API call to get the allocated blocks list is unsupported, therefore DPM must read all vmdk files (including empty blocks) and transfer all blocks to the DPM server, then write them to the vhdx file on the replica. This takes longer, however the storage consumed on the replica will be approximately the same due to optimization for zero block writes to the vhdx file on the replica.

**Delta Replication (DR):** There is no difference between recovery point synchronizations for VMs hosted on NFS vs VMFS. They are both accomplished by using the VMware API to ask for the changed blocks based on ChangeID. Only changed blocks will be transmitted to the DPM server replica volume.

**Consistency Check (CC):** This is basically the same as IR, only here the changed blocks will be transferred for CC of VMFS hosted VMs, but a full end-to-end read like traditional CC will need to be done for NFS hosted VMs. The CC will take longer for NFS hosted VM’s.

Moving a VM’s vmdk from an NFS disk to a VMFS disk and vice versa is supported, however a CC will be needed before protection can continue.

**Support for VM vMotion and migration to different storage**

DPM supports continuous protection of VMware guests, including moving VMs between hosts using vMotion or migrating a VM to different storage using storage vMotion. Moving a VM to a different folder or datacenter is also supported. These capabilities are possible because DPM uses the VMware backup APIs that support the scenarios.

**NOTE:** In UR11, if a DPM backup is in progress and vMotion is triggered, the backup will fail. This will be fixed in a later update for DPM. In the ideal situation, backup should prevent vMotion and vMotion should prevent backup. Currently if vMotion is in progress, backup will not start.

**Support for VM cloning**

If a VM is cloned, it will have the same UUID but it will have a unique InstanceUUID which is guaranteed to be unique across the datacenter. This ensures that DPM can continue protection of the original VM.

**Folder level protection under VMs and Templates**

VMware provides two types of folders: *Hosts and Clusters*, and *VMs and Templates*. VMs and Templates folders let you organize VMs in a way that suits your needs. For example, you may want to organize VMs based on applications they belong to or group VMs by department, or any number of other criteria.

DPM only supports VMs and Templates folders. DPM can be configured to protect individual VMs or protect all VMs under a folder by selecting the folder. A major benefit of adding folder level protection is that any new VMs added to the folder are protected automatically. DPM detects and configures protection for these VMs as part of a nightly maintenance job, so all VMs created will be configured for protection by end of the day. You can also run the DPM PowerShell command `start-autoprotection` at
any time to immediately initiate protection of newly added VM’s under an auto protected folder. When folder level protection is selected, the folder will show (Auto) in front of the name, as shown here:

Notes on folder level auto protection:

- You can rename protected folders or move any protected folder to a new location in the hierarchy and the VMs that are protected under that folder will remain protected.
- If you move protected VMs from under an auto-protect folder to different folder, DPM will continue protection of the VMs.
- The DPM UI will reflect the new folder name/location or the VM’s new location after being moved while enumerating vCenter when modifying the PG or when adding new protection.
- If you move all auto-protected VMs to different folders that are not located under the auto-protected folder, the original folder will lose its auto-protect status and any new VMs added under the folder will not be auto-protected. You need to re-enable auto-protect on that folder.

Excluding a VM from backup when in an auto-protected folder

To exclude one of more VMs in an auto-protected folder from protection, use vCenter and add a new custom attribute called **DisableDPMBackup** on the VMs you want to exclude from backup. After setting the **DisableDPMBackup** attribute on a VM, the VM will not be shown in the inquiry when creating or modifying a protection group, however if the attribute is set after an inquiry was already performed, that VM may still be shown. You will need to perform a refresh so it is removed from the DPM cache.

An example is shown below. In the screen shot, you can see the properties of a virtual machine called **VM01**. Under the annotations there is an *edit* link. To exclude the VM, you would click the link to bring up a new dialog box and add a new annotation called **DisableDPMBackup**, setting the value to **TRUE**.
Exclusion of VM in Auto Protection using VMware CLI

You can also set the custom attribute named `DisableDPMBackup` to `True` via a cmdlet in following way:

```powershell
#Create custom attribute named DisableDPMBackup if it is already there then skip this step:
$Server = Connect-VIServer -Server 10.10.10.10 -Protocol https -User admin -Password pass
New-CustomAttribute -Name "DisableDPMBackup" -TargetType VirtualMachine

#Get the VM object and set the value
$vm = Get-VM -Name "DoNotbackupThisVM"
Set-Annotation -Entity $vm -CustomAttribute "DisableDPMBackup" -Value "TRUE"
```
Setting the above value to anything other than TRUE will reverse the effect.

To download vSphere PowerCLI and get more info on cmdlets, see the links below.

vSphere PowerCLI Overview
Get-CustomAttribute
Remove-CustomAttribute
Set-CustomAttribute
Get-Annotation
Set-Annotation
New-CustomAttribute

Scale out protection of large private cloud deployments
A single DPM server can typically only protect approximately 800 average size VMs. To protect a large VMware deployment, multiple DPM servers can be leveraged to protect VMs managed by one or more vCenters. While multiple DPM servers can protect VMs deployed on the same vCenter, any given VM/folder can be protected by a single DPM server at any given time. VMs and folders that are already protected by one DPM server are not selectable by other DPM servers, as demonstrated below.
Once a folder is selected by a DPM server, all VMs and folders underneath this folder will be protected by the same DPM server automatically.

**NOTE:** This feature is only supported when protecting VMware ESXi hosts through vCenter, and is not supported when individual ESXi hosts are added to a DPM server for protection. Only a single DPM server should be used when protecting an ESXi host directly. ESX hosts do not support the custom attributes so they will not support scale out protection via vCenter.

The scale out feature is controlled by DPM by maintaining state information within vCenter for every VM or folder under protection. vCenter supports custom attributes called annotations for every object, and DPM leverages the annotations by creating a new global attribute called `DPMServer` which is then used to control which DPM server owns protection for a given folder or VM. Other DPM servers can query the custom attributes and find out if that folder or VM is already under protection, and if so, by which DPM server. If the `DPMServer` attribute contains a value for that object (folder/VM), DPM will show that the item is already protected and the DPM server protecting that item will be displayed.

Be aware that there is a delay between when a folder or VM is added to protection and when the `DPMServer` attribute is added to the object. The attribute is committed at Initial Replica (IR), Delta Replication (DR) and Consistency Check (CC) time. This means there is a window where another DPM server may attempt to protect the same folder or VM. This will not cause problems other than two DPM servers will be protecting the same objects. VMware change tracking will not be affected as each DPM server keeps track of its own reference points.

There may be times when a DPM server is no longer available, meaning that you need to re-protect a folder or guest using a different DPM server to continue protection. In such cases, use vCenter to clear the DPM server name in the `DPMServer` attribute for that object.

In our example below, the screen shot shows the properties of a VM called `ir-dr-cc-1disk`. Under the annotations there is an edit link, and clicking that link will bring up a new dialog box. To clear the existing DPM server name, find the name called `DPMServer` and clear it. This will allow another DPM server to protect it. **Do not remove the entire attribute or all scale-out tracking will be lost.** To clear the value, click in the Value box containing the DPM server name and remove the entry.

**NOTE:** Modifications of custom attributes on vCenter are not immediately committed in vCenter. A new backup or CC needs to be run against any guest under protection to commit attribute changes.
In addition to the DPMServer attribute, DPM also sets heartbeat on VCenter’s root folder with a custom field named LastRefreshTime_DPMServerName which is set to the UTC time in ticks.

Whenever the DPMServer property on a folder or VM is read, it will also read the last refresh time of that DPM server if the field does not exist. If it has a time value older than 15 days, it will be ignored. Access to this custom field is not locked which means multiple DPM servers can set the value at essentially the same time, and whatever value is set last remains. DPM reads those values at inquiry and updates them when a backup operation is run on that server. Because of this, there can be cases when a Protection Group is created but the attributes are not yet reflected on the vCenter server. Because of this, please be aware of the following:

- If protection of VMware VMs is done on one DPM server, and the DPM server does not protect any other VMs on that server, there will be no immediate backup operations. Because of this, custom attributes will not get updated on vCenter.
- If a DPM server is down or removed, it will take 15 days until the other DPM servers will ignore the attributes set by that DPM server.

There may also be scenarios where you want to protect the same VM via multiple DPM servers. In this case, and in the ones above, you may not be able to protect a folder or VM on vCenter on any other DPM server. You can use the following VMware cmdlets to overcome the issue via VMware PowerCLI.
1. To reset the value on a single object (folder or VM):

```powershell
Connect-VIServer -Server 10.10.10.10 -Protocol https -User admin -Password pass
$f = Get-Folder –Name “TestFolder”
Set-Annotation –Entity $f –CustomAttribute “DPMServer” –Value “”
```

2. To reset all the info for the DPM server (e.g. if the DPM server is removed):

```powershell
Connect-VIServer -Server 10.10.10.10 -Protocol https -User admin -Password pass
#Get custom attribute object
$ca = Get-CustomAttribute –Name “LastRefreshTime_DPMServername”
$ca
#Remove the last refresh time field so that all the values set by this dpm server will be ignored
Remove-CustomAttribute –CustomAttribute $ca
```

Back up VMs to various storage targets

DPM supports backup of VMware VMs to disk as well as to a Microsoft Azure cloud backup vault. DPM’s protection to disk and cloud are integrated into the protection workflow the same as other supported workloads. Secondary protection or tape backup for VMware workloads are not currently supported.

For all operational recovery scenarios like accidental deletion or corruption, disk backups can be used. Cloud backup can be leveraged for long-term retention or offsite backup requirements as documented in [Azure Backup for long term retention](#).
DPM can also do application consistent backup of Windows VMs and file consistent VM backup of Linux VMs. For this to work, you will need to install the VMware tools inside the guest.

**Important Note:** At the time of this writing, DPM will protect the VMware vhdk files by copying only allocated blocks inside the vhdk files and storing them on the DPM replica as a vhdx file. The size of the vhdx file is the same size as the protected vhdk file, however during recovery, DPM will restore the entire vhdk file including unallocated space. This means that the restored VM will require more physical disk space on the selected datastore than what was originally used.

**Example:** Let’s say that a VM has a 40GB virtual disk attached and the allocated space inside the vhdk file is only 23GB. After protecting the VM, the DPM replica will have a 23GB vhdx file. When the restore is done, the resulting vhdk file will not be the original 23GB, but rather the 40GB size of the virtual disk.

**Unsupported scenarios**
DPM VMware protection does not support the following scenarios:

1. Raw Device Mapping (RDM) pass thru disks can be configured in either physical compatibility mode or virtual compatibility mode. Physical RDM (PRDM) is not supported, however Virtual RDM (VRDM) is supported. More about Raw Device Mapping can be found here.
2. Clustered VMs are supported, however VMs hosted on shared disk clusters are not supported. Change tracking on shared disks is not supported by VMware.
3. DPM cannot detect or protect VApps.
4. DPM currently cannot protect VMware VMs to tape or a secondary DPM server.
5. Manual replica creation is not supported. You must either let DPM create the initial replica at the time of protection or schedule it to run later.
6. DPM can protect VMs with snapshots, however the snapshots are not backed up and are not restored during a VM recovery. If the snapshot was created before protection, DPM cannot protect that VM because VMware does not support enabling change tracking for any VM that has existing snapshots. A work around is to delete the existing snapshots.
7. The Microsoft Operations Manager console does not currently support monitoring VMware data sources, however they will show up under the All Datasources view. VMware protection alerts will only show under All Alerts. You can modify the OpsMgr management pack (MP) by making a custom view and overriding the DPM MP.

**Recovering VMs**
DPM supports both Original Location Recovery (OLR) and Alternate Location Recovery (ALR).

**Original Location Recovery (OLR)**
Protected VMs can be recovered to their original location which will overwrite the existing VM. Original Location Recovery (OLR) is supported only when the VM is still present and the VM disk configuration did not change from backup time. This is done by selecting Original Location Recovery as shown below.
DPM will perform the following when doing an Original Location Recovery (OLR):

1. Check to see if the number of disks on the VM being recovered matches the number of disks in the recovery point.
2. Check to see if the UUID of the disks and the paths match.

If either of these checks fail, the recovery will fail with error `VMConfigMismatched`.

DPM will always transfer the whole disk; it does not matter if the original disk was thick or thin provisioned. If the VM was deleted and you attempt to restore to the original location, the recovery will fail with the below error and failed job details:
Type: Disk recovery  
Status: Failed  
Description: DPM encountered error from VMware server 172.29.9.219 with Fault - VMNotFound (ID 33614 Details: Internal error code: 0x80990EF0)  
More information  
End time:  
Start time:  
Time elapsed:  
Data transferred: 0 MB (0 bytes)  
Source details: testbox01  
Target details: testbox01 on 172.29.9.219  
Cluster node:  

If the Datastore does not have enough free space for the recovery, the failed job details will show an error similar to the following:

Type: Disk recovery  
Status: Failed  
Description: DPM encountered error from VMware server 172.29.9.219 with Fault - NoDiskSpace (ID 33614 Details: Internal error code: 0x80990EF0)  
More information  
End time:  
Start time:  
Time elapsed:
Alternate Location Recovery (ALR)

If the original VM is missing, or you do not want to disturb the original VM, the VM can be recovered to an alternate location. When recovering to an alternate location, DPM will need certain parameters as shown below. Each parameter is enumerated and selectable using the browse button. The screen shot below shows an alternate location recovery with the parameters filled in.

Example summary page with final details:
When a VM is recovered to an alternate location, DPM will create a new virtual machine and append a “-Recovered” to the name of the VM and the underlying files to help in differentiating from the original VM.
Individual vmdk file recovery
There may be times when you want to restore a single vmdk file instead of an entire VM. With Hyper-V protection, this is possible because the VM’s files are stored natively as vhd or vhdx files. Unlike Hyper-V protection, it is not possible to restore individual vmdk files associated for a VMware virtual machine. You can see in the screen shot below that the option to recover an individual vmdk file is not available.

This is because the vmdk file is stored as a vhdx file on the DPM server so that it can be mounted when performing Item Level Recovery for Windows VM’s. When restoring a VMware virtual machine, DPM will mount and read the vhdx file and write the data to the vmdk file on the ESX server.

Item Level Recovery (ILR)
If the protected VM is a Windows VM, individual files or folders inside the VM can be recovered using DPM’s Item Level Recovery (ILR) capability. To do this, click on Recovery, select the corresponding vmdk file, then select the files to recover as shown below. This will mount the corresponding vhdx file and copy it to the destination location.

PowerShell commands
VMware operations can also be achieved using PowerShell commands. Below is a list of PowerShell commands that have been added to support VMware protection. All examples will follow these commands:
Output

ServerName : DPM01
ClusterName :
Domain : fabrikam.local
ServerProtectionState : NoDatasourcesProtected

ServerName : 172.29.9.219
ClusterName :
Domain :
ServerProtectionState : HasDatasourcesProtected

ServerName : FBKMDC01
ClusterName :
Domain : fabrikam.local
ServerProtectionState : NoDatasourcesProtected

Get-DPMVMWareInventory
VMware’s folder infrastructure and other related VMware infrastructure can be retrieved using the Get-DPMVMWareInventory PowerShell command.

Get-DPMVMWareInventory [-ProductionServer] <ProductionServer> [-Async] [-Inquire] [-Tag <Object>] [ <CommonParameters>]

Output
Returns the VMWareRecoveryInfra object. The VMWareRecoveryInfra object includes the following:

VMWareRecoveryInfra
{
    VMWareFolder RootFolder;
    VMWareComputeResource ComputeResources[];
}

VMWareFolder
{
    VMWareFolder Childfolders[];
}

VMWareComputeResource
{
    VMWareDataStore VMWareDataStore[];
    VMWareResourcePool RootResourcePool;
}
VMWareResourcePool
{
    VMWareResourcePool Childresourcepools[];
}

Example
get-dpmvmwareinventory -productionserver $ps[1] -inquire
(get-dpmvmwareinventory -productionserver $ps[1] -inquire).rootfolder.childfolders | fl *

ChildFolders      : {host, vm}
IsChildOfVMFolder : False
Name              : CSS Lab LC
RefId             : datacenter-21
ParentRefId       : group-d1
Type              : Datacenter

ParentObject      : Microsoft.Internal.EnterpriseStorage.Dls.UI.ObjectModel.OMCommon.VMWareFolder

Auto Protection of a folder
To protect VMs in a folder automatically, use the **Set-DPMAutoProtectIntent** PowerShell command:

**Set-DPMAutoProtectIntent** [-ProtectionGroup] <ProtectionGroup> [-VMWareFolder] <VMWareFolder> [-AutoProtectIntent] <AutoProtectionIntent> {Enable | Disable} [-ProductionServer] <ProductionServer>

Alternate Location Recovery (ALR)
If a VM needs to be recovered to an alternate location, DPM needs to know various parameters like target host, etc. In this process, first you need to get VMware Inventory using the **Get-DPMVMWareInventory** command as shown above, then using that inventory object, do an ALR using the following PowerShell command.

**New-DPMMRecoveryOption** [-TargetServer] <string> [-DPMLibrary <Library>] [-RecoverToReplicaFromTape <Boolean> -VMWareVM [-VMWareTargetFolder <VMWareFolder>] [-VMWareTargetResourcePool <VMWareResourcePool>] [-VMWareTargetComputeResource <VMWareComputeResource] [-VMWareTargetDatastore <VMWareDatastore>] [<CommonParameters>]

Output
VMWareVMRecoveryOptions

Example
$inventory = Get-DPMVMWareInventory –ProductionServer $ps

Now you can do $inventory.RootFolder.ChildFolders[0].ChildFolder[0] to get access to various object of inventory.
Get-DPMCredential
This will return a DPM credential object that can be used as an input for subsequent commands.

Get-DPMCredential –Name <name>

Example
PS C:\Program Files\Microsoft System Center 2012 R2\DPM\DPM\bin> Get-DPMCredential

<table>
<thead>
<tr>
<th>CredName</th>
<th>Description</th>
<th>UserName</th>
<th>LastModified</th>
</tr>
</thead>
<tbody>
<tr>
<td>superman</td>
<td>MS ESXi server</td>
<td>root</td>
<td>6/10/2016 6:31:00 PM</td>
</tr>
<tr>
<td>vCenter Server VM1</td>
<td>vCenter Server VM1</td>
<td>root</td>
<td>6/10/2016 6:32:50 PM</td>
</tr>
<tr>
<td>vCenter2Credential</td>
<td>vCenter2 Password</td>
<td>root</td>
<td>6/3/2016 10:39:44 PM</td>
</tr>
<tr>
<td>VPXUser</td>
<td>Test User</td>
<td>vpxuser</td>
<td>6/21/2016 9:48:07 PM</td>
</tr>
</tbody>
</table>

PS C:\Program Files\Microsoft System Center 2012 R2\DPM\DPM\bin> Get-DPMCredential -name superman

<table>
<thead>
<tr>
<th>CredName</th>
<th>Description</th>
<th>UserName</th>
<th>LastModified</th>
</tr>
</thead>
<tbody>
<tr>
<td>superman</td>
<td>MS ESXi server</td>
<td>root</td>
<td>6/10/2016 6:31:00 PM</td>
</tr>
</tbody>
</table>

Add-DPMCredential
This command is used to add a new credential to DPM which can be used for authenticating to a VMware server.

Add-DPMCredential [-Name] <string> [-PSCredential] <pscredential> [[-Description] <string>] [<CommonParameters>]

Add-DPMCredential [-Name] <string> [-UserName] <string> [-Password] <securestring> [[-Description] <string>] [<CommonParameters>]

Example
PS C:\Program Files\Microsoft System Center 2012 R2\DPM\DPM\bin> add-dpmcredential -name batman -description pstest -username administrator

cmdlet Add-DPMCredential at command pipeline position 1
Supply values for the following parameters:
Password: ********

<table>
<thead>
<tr>
<th>CredName</th>
<th>Description</th>
<th>UserName</th>
<th>LastModified</th>
</tr>
</thead>
<tbody>
<tr>
<td>batman</td>
<td>pstest</td>
<td>administrator</td>
<td>6/24/2016 11:03:20 PM</td>
</tr>
</tbody>
</table>
Remove-DPMCredential
This command removes a given credential. Note that a credential can be removed only if no VMware server is using it for authentication.

Remove-DPMCredential [-Name] <string> [CommonParameters]

Example
Remove-DPMCredential -name batman

Update-DPMCredential
This updates a given credential.

Update-DPMCredential [-Name] <string> [-PSCredential] <pscredential> [[-Description] <string>] [CommonParameters]

Update-DPMCredential [-Name] <string> [-UserName] <string> [-Password] <securestring> [[-Description] <string>] [CommonParameters]

Update-DPMCredential –Name <name> -UserName <user> -Password <password>

Update-DPMCredential –Name <name> -UserName <user>

Update-DPMCredential –Name <name> -Password <password>

Example
PS C:\Program Files\Microsoft System Center 2012 R2\DPM\DPM\bin> update-DPMCredential -name batman-username newuser -description newdesc

cmdlet Update-DPMCredential at command pipeline position 1
Supply values for the following parameters:
Password: *****

<table>
<thead>
<tr>
<th>CredName</th>
<th>Description</th>
<th>UserName</th>
<th>LastModified</th>
</tr>
</thead>
<tbody>
<tr>
<td>batman</td>
<td>newdesc</td>
<td>newuser</td>
<td>6/24/2016 11:25:42 PM</td>
</tr>
</tbody>
</table>

Add-DPMProductionServer
This PowerShell command adds a given production server to a DPM server.

Add-DPMProductionServer –Name <servername> -CredName <dpmcred>

Parameters: <servername>: string  <dpmcred>: string

Remove-DPMProductionServer
Remove a given production server from a DPM server.

Remove-DPMProductionServer –ServerId <ServerId>
Update-DPMProductionServer
Update a given production server settings.

Update-DPMProductionServer –Action <Credential> –ServerId <ServerId> -CredName <credname>

Parameters: <Credential>: enum <ServerId>: Guid <credname>: string

Troubleshooting
Since there is no DPM agent installed on the VMware host, most errors will be recorded in the DPMRA and MSDPM error logs on the DPM server. That is the first place to look for any DPM backup or restore failures as VMware errors will be included in the DPMRA logs.

VMware logs can be gathered using the vSphere client. After connecting to the ESX host you can export the logs under System Logs, then export system logs.
Problem: DPM does not enumerate or display one or more VMs to protect
It is possible that one or more VMs were excluded from auto-protection and have the DisableDPMBackup attribute set. Remove the DisableDPMBackup attribute from the VM as described in the section titled “Excluding a VM from backup when in an auto-protected folder” above.

Problem: Alternate Location Recovery (OLR) fails or causes console crashes
During a recovery to an alternate location, DPM converts the VMware VMs configuration file (called a ConfigSpec) captured during backup to a ConfigInfo object which is used to perform a restore to an alternate location. The mapping between ConfigSpec and ConfigInfo is performed by DPM as there is no method or API from VMware to create it. There may be rare cases when this mapping does not work which will cause the VM restore to fail or cause a DPM crash. Other symptoms are that the VM might not boot, or that some virtual hardware is missing from the VM. Look in the dpmra errlog and search for ConvertConfigInfoToSpec. If you find that then you know that the mapping failure was the cause.

Addendum
Steps for importing vCenter certificates into DPM for certificate authentication
The VMware article below lists the step by which you can install and configure certificate on vCenter Server:

To install the cert on a DPM server you would follow the procedure in the following article:
The download button is not there but you can use the following PowerShell script to download the certificate, then continue with the steps.

NOTE: Replace `https://vcenterserver.fabrikam.com` with the vCenter server name.

```powershell
$webRequest = [Net.WebRequest]::Create("https://vcenterserver.fabrikam.com/")
try { $webRequest.GetResponse() } catch {}
$cert = $webRequest.ServicePoint.Certificate
$bytes = $cert.Export([Security.Cryptography.X509Certificates.X509ContentType]::Cert)
set-content -value $bytes -encoding byte -path "$pwd\vcentervm1.cer"
```